

Cybersécurité, culture d'entreprise

Avec cette déclaration lors de l'édition 2025 du Cyber Africa Forum, à Cotonou, Uche Ofodile, CEO de MTN Bénin, en interpelle plus d'un.

« La cybersécurité n'est plus un sujet purement technique, comment la transformer en une culture d'entreprise ? »



Cybersécurité, culture d'entreprise

— Par Perpétus Jacques Houngho

La Cybersécurité a muté dans un changement de paradigme. Lors de l'édition 2025 du Cyber Africa Forum, à Cotonou, Uche Ofodile, CEO de MTN Bénin a déclaré « La cybersécurité n'est plus une affaire de spécialistes IT. C'est devenu une culture d'entreprise ». Un an après le Cyber Africa Forum de Cotonou, la question reste entière de savoir comment y parvenir, comment diffuser la cybersécurité dans l'entreprise.

Comprendre la culture d'entreprise

Au nombre des éléments les plus fréquemment utilisés pour une définition de la culture d'entreprise, on retrouve les valeurs, les pratiques, les croyances, les normes et les comportements qui caractérisent l'entreprise. Ces éléments sont constitutifs de l'ADN de l'entreprise à travers trois piliers fondamentaux : la raison d'être (pourquoi elle existe), la vision (où elle va) et les valeurs (comment elle agit). Performance, innovation et éthique sont au nombre des valeurs les plus référencées.

Intégrer la cybersécurité dans l'ADN de l'entreprise

Le point de départ est que le dirigeant de l'entreprise prenne la mesure de sa responsabilité. De nos jours, l'infrastructure informatique est complexe, distribuée, basée sur le cloud, avec une adoption rapide (maîtrisée ou imposée) de l'intelligence artificielle. Dans ce contexte, il devient impératif que le dirigeant comprenne, quand bien même le discours du Responsable de la Sécurité des Systèmes

d'Information n'est pas assez explicite, que les enjeux sont en termes de réduction des risques, de prévention des pertes, de continuité des activités, de protection de la valeur actionnariale. Une fois cette prise de conscience réalisée, le dirigeant adopte une approche structurée, qui commence par la gouvernance de la cybersécurité, qui intègre la formation et la sensibilisation de tout le personnel, qui prend appui sur des solutions technologiques intelligentes. Cette approche structurée se traduit par un ensemble d'attitudes et de comportements auxquels adhère le dirigeant d'entreprise. Ses capacités de leadership en sont plus renforcées par exemplarité et implication active.

La norme ISO 27001 est un cadre organisationnel et processuel qui apporte de nombreuses solutions dans cette approche structurée. Des éléments d'attitudes et de comportements sont proposés ci-dessous pour composante de cette approche.

La référence à la norme ISO 27001 peut prêter à sourire si l'on considère que cela revient à « utiliser un marteau pour tuer une mouche ». Mais ce n'est évidemment pas le cas. Quel que soit l'outil utilisé pour tuer la mouche, il requiert de l'énergie, de la rapidité et de la précision. En cela, la norme ISO 27001 est très attachée au principe fondamental de proportionnalité. Les actions doivent être justifiées par une analyse des risques objective afin d'éviter des coûts ou des freins opérationnels inutiles. La certification n'est pas une obligation; il convient d'abord de raisonner en termes d'avantages opérationnels, d'atouts commerciaux et de gains de productivité grâce à l'amélioration continue des processus.

Gouvernance de la cybersécurité

Le dirigeant pilote la conception de la politique de sécurité de l'information, il veille à une attribution conséquente des rôles et des responsabilités, il supervise la communication de la politique de sécurité de l'information et il coordonne l'établissement d'objectifs et de plans d'amélioration continue.

Quelques exigences de cette norme ISO 27001 permettent de bien installer le dirigeant dans ce rôle de gouvernance de la cybersécurité :

- La Clause 4, intitulée « Contexte de l'organisation », point de départ indispensable pour bâtir un Système de Management de la Sécurité de l'Information (SMSI) efficace, exige que le dirigeant identifie les enjeux internes et externes, les parties intéressées et leurs attentes, et qu'il définisse le périmètre du SMSI.
- La Clause 5, intitulée « Leadership », exige que la direction générale s'implique activement dans la mise en œuvre du système de management de la sécurité de l'information (SMSI) plutôt que de s'en remettre uniquement au service informatique.
- La Clause 6, intitulée « Planification », définit comment anticiper les risques et atteindre les objectifs de sécurité.

Se conformer à ces trois exigences est loin d'être une évidence. Il s'agit pour le dirigeant de comprendre les vulnérabilités spécifiques à son organisation et les menaces à son activité, d'identifier les processus critiques, de définir les priorités. C'est une démarche composée de plusieurs étapes itératives, elle s'inscrit donc dans le temps.

Formation et sensibilisation

Exemplarité et posture permettent au dirigeant de donner le "ton au sommet". Non seulement il pilote la conception et la mise en œuvre des activités de formation et de sensibilisation, mais encore il y participe lui-même.

La mise en œuvre du Système de Management de la Sécurité de l'Information (SMSI) requiert fondamentalement l'implication de tout le personnel de l'entreprise. Il est important de procéder avec des programmes réguliers qui associent formations, simulations, recours à des directives claires et précises dans les tâches quotidiennes. Les tests des plans de sauvegarde, des plans de continuité d'affaires, des plans de reprise après sinistre participent à cette démarche de création des réflexes qui permettront de nourrir cette culture d'entreprise.

La Clause 7, intitulée « Support », est, à cet égard, d'un grand apport. Elle exige que l'entreprise fournisse des ressources, assure la compétence du personnel, développe la sensibilisation, gère la communication et maintienne des informations documentées.

Solutions technologiques intelligentes

Les solutions technologiques intelligentes sont, à bien des égards, le domaine réservé des spécialistes. Mais de par son attitude proactive (moteur du changement), le dirigeant d'entreprise ne subit pas la technologie; il ne se contente pas de déléguer aveuglément cette tâche. Il inspire son équipe, il conduit les changements, il pilote la stratégie face aux innovations.

La question des solutions technologiques intelligentes est déjà couverte par la Clause 7, intitulée « Support ». Cette Clause 7 énonce spécifiquement une liste de domaines dans lesquels elle attend des actes du dirigeant d'entreprise. Il s'agit des cinq domaines ci-après :

- 7.1 Ressources

L'entreprise doit déterminer et fournir les ressources nécessaires. Il est aisé de comprendre que ces ressources couvrent les ressources humaines, les ressources financières, les ressources organisationnelles et aussi les moyens techniques mis à disposition. Au nombre de ces moyens des solutions technologiques intelligentes permettent aux divers responsables à plusieurs niveaux de gérer efficacement les risques, la documentation, les opérations d'appui du leadership, les opérations de mise en œuvre, les changements, le suivi et l'évaluation en continu. Chaque niveau d'intervention requiert des solutions technologiques intelligentes spécifiques. C'est la responsabilité du dirigeant d'entreprise de veiller à ce que prolifération et mise en œuvre en silos ne viennent gâcher l'orchestration harmonieuse de l'ensemble.

- 7.2 Compétences / 7.3 Sensibilisation

En partant du fait que plus de 62 % des failles de sécurité proviennent d'une erreur humaine¹, il est souvent répété que le facteur humain est le maillon faible de la chaîne de sécurité. C'est justement la responsabilité du dirigeant d'entreprise d'inverser cette approche et d'apprécier son équipe comme étant un des maillons forts de la chaîne. Le renforcement de la compétence du personnel constitue l'une de ses priorités pour réduire les risques de cybersécurité et améliorer la résilience.

Les solutions technologiques intelligentes sont aujourd'hui nombreuses pour couvrir formation, sensibilisation et plaidoyer. De nombreux modèles de formation à la cybersécurité visent à préparer les professionnels à faire face à des attaques sophistiquées et à gérer les risques liés à la sécurité. Compte tenu de l'évolution rapide du paysage des menaces, ces modèles de formation mettent l'accent sur des simulations dynamiques, pratiques et adaptées à chaque rôle. Cette évolution est principalement motivée par la nécessité de lutter contre les menaces liées à l'intelligence artificielle et de pallier la pénurie de compétences dans le domaine de la cybersécurité.

- 7.4 Communication

En matière de sécurité de l'information, une communication assumée et intelligente implique d'apporter les bonnes réponses aux questions de quoi (contenu), quels (forme et format), qui (communiquant), à qui (cible), comment (processus) et quand (fréquence). Les solutions technologiques intelligentes, telles que les plateformes de communications unifiées, les messageries instantanées dopées à l'IA et la visioconférence intelligente, centralisent les échanges et automatisent les tâches répétitives. Ces solutions constituent des leviers pour l'entreprise, elles transforment les lieux de travail en environnements dynamiques et connectés pour stimuler la productivité des équipes.

- 7.5 Informations documentées

Un système de management de sécurité de l'information basé sur la norme ISO 27001 s'articule essentiellement sur l'information documentée. L'entreprise se doit donc de mettre en œuvre une documentation vivante et intégrée à sa culture de l'entreprise. Une telle documentation lui permet de mieux s'organiser, de formaliser ses processus et de définir la manière dont chacun doit agir pour garantir la cohérence, la sécurité et la conformité.

Le dirigeant d'entreprise veille à ce que les solutions de gestion documentaire mises en œuvre disposent de fonctionnalités telles que le traitement Intelligent des Documents, des systèmes de gestion de contenu, des outils de recherche avancée, etc. La documentation ISO 27001 est un véritable outil de pilotage et de confiance au service de l'entreprise.

Intégrer la cybersécurité dans l'ADN de l'entreprise signifie que le dirigeant d'entreprise a imprégné la cybersécurité dans la raison d'être de l'entreprise, sa vision et ses valeurs. Il a adopté des attitudes et des comportements qui lui permettent de :

- **piloter la conception de la politique de sécurité de l'information, veiller à une attribution conséquente des rôles et des responsabilités;**
- **piloter la conception et la mise en œuvre des activités de formation et de sensibilisation, et**

¹ Rapport Data Breach Investigations Report – DBIR – 2026, <https://www.verizon.com/business/fr-fr/resources/reports/dbir/>

- y participer en personne;
- piloter la stratégie face aux innovations.

C'est à lui qu'incombe la définition de la vision et sa transformation en une force d'adhésion collective. La norme ISO 27001 est un cadre organisationnel et processuel qui apporte au dirigeant d'entreprise de nombreuses solutions dans cette approche structurée.